ABSTRACT OF THE DISCLOSURE

A system and method for secure computing. The system includes a processor, one or more secured assets coupled to the processor, and security hardware. The processor is configured to operate in various operating modes, including a secure operating mode. The security hardware is configured to control access to the secured assets dependant upon the operating mode of the processor. The security hardware is configured to allow access to the secure assets in the secure operating mode, preferably only in the secure operating mode. The method includes switching the computer system between operating modes, while allowing or restricting access to the secured assets based on the operating modes. The second operating mode comprises a secure operating mode. The method restricts access to the secured assets in the first operating mode and permits access to the secured assets in the secure operating mode.